Akamai

4 Reasons Your Business Needs Zero Trust Security

Table of contents

Introduction

As attackers become more sophisticated, ransomware groups proliferate, and advances in technology introduce new vulnerabilities, organizations are increasingly turning to a Zero Trust security model. At its core, this approach eliminates the implicit trust of users, applications, and devices, which was a central tenet of previous approaches to security. In practical terms, there are four key scenarios in which an organization will benefit from a Zero Trust security model — a ransomware attack against your company, a move to remote work, a need to secure your cloud environment, or an upcoming audit.

These scenarios are the result of recent trends — the increase in ransomware attacks, the move to a hybrid workforce, the migration to cloud computing, and increased demands from security audits — which require a security approach that is based on verifying identity, regardless of location, and takes proactive measures when dealing with breaches. Zero Trust is the only approach that requires strong user identity to access data and provides proactive mitigation once an attack has occurred.

Implementing a Zero Trust strategy may seem overwhelming for already overworked security teams, but it doesn't have to be. By taking a phased approach and focusing on quick wins, you can decrease some of the complexity and risk associated with traditional security solutions and improve your security posture.

You don't have to rip and replace your existing tech to get started. Start by aligning your Zero Trust investments with your most pressing business needs. Opt for a trusted Zero Trust vendor over vendors that have evolved overnight and rebranded their older solution as Zero Trust. Strongly consider a vendor that can combine multiple elements of Zero Trust security (Zero Trust Network Access, DNS firewall, microsegmentation, etc.) under a single platform. Whatever your reason for adoption, Zero Trust will allow you to realize business agility, cost optimizations, and tool consolation, and will improve your overall operations.

Top 4 reasons organizations turn to Zero Trust

- The increase of ransomware attacks
- The hybrid workforce
- The adoption of cloud computing resources
- Rigorous compliance requirements

01

The increase in ransomware attacks

Boost your ransomware protection

In the last few years, ransomware attacks have disrupted organizations around the globe, from hospitals and banks to pipelines and other critical infrastructure. In fact, **Cybersecurity Ventures** predicts that ransomware will cost its victims approximately US$265 billion annually by 2031. It predicts that ransomware perpetrators will launch a new attack (on a consumer or business) every two seconds as they progressively refine their malware payloads and related extortion activities.

Without a Zero Trust strategy, ransomware groups can take advantage of the following weaknesses:

- ☑ Implicit trust for users, applications, and networks that allows attackers who have managed to breach the network to move laterally and spread malware
- ☑ Overly permissive access policies that allow infections that can then be used to inject ransomware
- ☑ Systems that trust a password alone, which provide an opportunity for credential theft

How Zero Trust helps

Companies who put in place a Zero Trust architecture, have access control policies, and use microsegmentation minimize the damage that such an attack can cause. Attackers not only find it more difficult to breach the system in the first place, they're limited in their ability to expand.

How Akamai breaks the ransomware kill chain

A ransomware attack typically involves an initial infection, lateral movement, and data exfiltration and encryption. With Zero Trust, organizations can address each step as it happens — or even before it happens.

> "Ransomware will attack a business, consumer, or device every two seconds"

by 2031, according to the Who's Who in Ransomware report 2023 from Cybersecurity Ventures

Initial infection

The Akamai Guardicore Platform helps prevent an attack from spreading beyond the initial point of entry while Akamai MFA protects users from having their credentials stolen and abused.

Lateral movement

The Akamai Guardicore Platform reduces propagation paths and helps prevent lateral movement. Akamai Guardicore Access limits the attacker's ability to move to infect the application they were hoping to exploit. Akamai Hunt detects and mitigates evasive advanced threats in your network.

Data exfiltration and encryption

The Akamai Guardicore Platform limits access to critical applications, keeping attackers from accessing sensitive data within a compromised network. Akamai Secure Internet Access Enterprise blocks requests to phishing sites and command and control sites. Finally, Akamai Hunt detects anomalous behavior, preventing attackers from encrypting valuable data that can be ransomed.

02

The hybrid workforce

Secure the new hybrid workforce

Securing a new, hybrid workforce that has grown and expanded because of the COVID-19 pandemic is more challenging when organizations rely on outdated security tools, such as firewalls and VPNs. When remote access VPNs were first introduced some 30 years ago, everything was different — the internet was in its infancy, applications were running in the data center, and there were far fewer users connecting from remote locations. Continuing to authenticate users with a VPN and then giving them access to the entire network increases the attack surface and opens the door to many of the zero-day vulnerabilities that come with legacy VPNs. Any user with the necessary credentials can log on to a corporate VPN and, once inside, move laterally throughout the network and access the resources the VPN was meant to protect.

How Zero Trust helps

Based on the principle of least-privilege access, Zero Trust assumes that no user or application should be inherently trusted. Zero Trust Network Access (ZTNA) takes a completely different approach than VPNs to securing access for remote workers. Instead of risking the entire network, users are connected directly to only the applications and data they need, preventing the lateral movement of malicious users with overly permissive access to sensitive data and resources. In the event of a breach, an effective Zero Trust microsegmentation solution can segment the internal network so the breach doesn't spread and damage other parts of the network. According to **Gartner**, at least 70% of new remote access deployments will be served mainly by ZTNA instead of VPN services by 2025 — up from less than 10% at the end of 2021.

> “According to Gartner, at least 70% of new remote access deployments will be served mainly by ZTNA instead of VPN services by 2025 — up from less than 10% at the end of 2021.”

How Akamai facilitates hybrid and remote work

Akamai's comprehensive Zero Trust platform meets the needs of your hybrid workforce. Benefits include:

Reduced risk

Akamai directly connects the right user to the right application, reducing the attack surface and limiting lateral movement.

Improved user experience

Remote users enjoy access to resources regardless of application, device, or location, eliminating the need for connection to and disconnection from the VPN.

More agility

Since Akamai's solution is consumed as a service, organizations have no hardware to deploy and don't need to worry about scaling as demands increase, which reduces cost and complexity.

03

The adoption of cloud computing resources

Ease cloud migration

Organizations are moving their apps to the cloud to achieve flexibility and agility and to modernize their infrastructure. However, these cloud environments are expanding the attack surface and introducing new security requirements. Integrations among different clouds and on-premises environments can break applications and put security at risk. When organizations attempt to migrate their applications to the cloud using traditional network constructs — VPNs and firewalls — they often face an increased risk of lateral threats, poor scalability, and high costs. Even after the migration is complete, assets still need to be secured and users must be authenticated based on role permissions. Users of cloud infrastructure typically have greater access to resources, services, and management entitlements than they might otherwise have with on-premises environments, which introduces additional risk and the potential for disruption.

How Zero Trust helps

Zero Trust strategies facilitate migration to the cloud. Zero Trust removes the implicit trust inherent in many cloud-based applications, particularly third-party applications, that can introduce vulnerabilities. Zero Trust solutions ensure that organizations can more easily deploy their cloud-based applications with stronger protections. Some of the benefits of deploying Zero Trust for the cloud include:

☑ Better visibility into assets and risks

☑ Reduced attack surface with Zero Trust segmentation and least-privilege access to cloud resources

☑ Modernized network infrastructure that provides speed and agility

☑ Reduced operational cost and complexity

How Akamai improves cloud migration

Akamai’s Zero Trust solutions can help you automatically migrate your assets and their respective policies. There is no downtime and no disruption to the business. Akamai delivers:

Greater visibility

With a better understanding of app dependencies, you can create effective cloud segmentation policies to reduce the attack surface and minimize risk.

Zero Trust Network Access

Users can only connect to the apps they are authorized to access based on strong authentication.

Threat hunting

Akamai’s dedicated team of threat hunters continuously searches for anomalous attack behaviors across cloud environments and notifies Akamai customers of any risk to their network.

04

Rigorous compliance requirements

Simplify compliance and reduce risk

While security leaders know that meeting compliance requirements does not equal a truly secure organization, security audits are still top of mind for executive teams. They know that failed audits can lead to major business disruptions and impact the bottom line. A compliance assessment is one of the most time-consuming and resource-draining activities for security teams. Additionally, the move to perimeterless digital environments and the prevalence of remote work have made compliance even harder. Organizations typically need to isolate their environments and ringfence their regulated assets to meet compliance standards, such as the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), and the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Organizations also need to accommodate remote users, corporate on-premises users, partners, suppliers, and more, which makes the perimeter of an organization's environment almost impossible to define. As security teams prepare for audits in which access control is a main determiner of success, they must address the following questions:

- How can we restrict access to sensitive information to authorized users only?

- How can we scope the audit environment?

- How can we make the audit process simpler and less chaotic?

How Zero Trust helps

Fortunately, a Zero Trust approach can help address all these questions and more. The two key pillars of Zero Trust — the ability to verify explicitly and to support least-privilege access — greatly simplify the process of compliance. Organizations can isolate their regulated assets from other traffic in their data center or the cloud and allow access based on identities, regardless of location. Enhanced visibility shows what's flowing in and out of their regulated environment and helps identify what's in scope. This greatly reduces the complexity and cost of the audit and makes the auditor's life easier.

How Akamai facilitates compliance

Akamai's comprehensive Zero Trust portfolio helps you prepare for every audit — whether PCI DSS, HIPAA, International Standards Organization (ISO), Sarbanes–Oxley (SOX), or any other framework. Akamai Enterprise Application Access controls access by third parties to sensitive personal information, meeting General Data Protection Regulation (GDPR) requirements. Akamai Guardicore Segmentation improves the understanding of regulated assets under PCI DSS, isolates clearinghouse functions to address HIPAA, and restricts internet access and isolates critical systems to meet SWIFT regulations. Akamai MFA protects HIPAA patient information from attackers who have obtained passwords to healthcare systems, and it bolsters SWIFT compliance by preventing the compromise of credentials.

Global bank achieves SWIFT compliance in two weeks

External regulators required one of Akamai's clients, a global bank, to ringfence all its critical applications to meet the requirements of SWIFT for a secure transfer of money between financial institutions. Typically, an application like this requires more than 100 servers deployed in different locations, including bare-metal and virtual servers. On average, this process could take a bank of its size between 8 and 12 months to plan and execute because it would have to create a virtual local area network (VLAN) for the segment across multiple locations. Figuring out the dependencies of the SWIFT application and making sure the ruleset was correct and didn't break anything would have only added to the timeline. Meanwhile, the project would also require purchasing new firewall equipment. And because the SWIFT application is critical to the banking business, the bank could not tolerate downtime. All in all, the segmentation project was expected to require a massive effort by many people. But, with Akamai, the whole process took just one security engineer approximately two weeks to complete; it did not require any network changes and the bank avoided any application changes or downtime.

Simplify and accelerate compliance

Global bank

- Need to ringfence SWIFT application
- Complex environment with bare-metal, VMware, and OpenStack servers

Traditional segmentation

- Hard to define segments across complex infrastructure
- No visibility into applications and dependencies
- Requires downtime

Time: 8–12 months

People: At least 5

Akamai Guardicore Segmentation

- Completed SWIFT application mapping in hours
- Segmentation policies automatically suggested and fine-tuned
- No need to purchase and deploy new hardware and firewalls
- No downtime

Time: 2 weeks

People: 1 architect

Learn more about meeting your business needs with the Akamai Zero Trust Portfolio

Learn more